Walgreens Boots Alliance

Policy number:	**WBA.GESP.1**
Policy title:	**Global end user security**
Issue date:	**4 October 2019**
Version:	**3.1**
Owner:	**WBA Vice President, IT Governance, Risk & Compliance**
Description:	**This policy describes the information and data security requirements for all facilities, systems, networks, data (electronic and non-electronic) and devices within Walgreens Boots Alliance ("WBA").**

Table of contents

This policy has been prepared by Walgreens Boots Alliance, Inc. and its affiliates ("WBA") for internal purposes only. All WBA internal policies are kept under ongoing review and are subject to change at any time, and must not be redistributed to third parties without our express permission.

1. Purpose

The purpose of this Global End User Security Policy ("GESP") is to highlight the information and data security requirements for all facilities, systems, networks, data (electronic and non-electronic) and devices within Walgreens Boots Alliance ("WBA"). For the purpose of this policy:

- Walgreens Boots Alliance ("WBA") means the Company, and its Divisions, Businesses and the Corporate functions; and
- IT Leadership is any individual responsible for an information technology division, shared services technology function or a cross-divisional function. E.g. Chief Information Officer (CIO), Divisional Chief Information Officer (DCIO), Information Security Officer, Vice President, equivalent, or designee.

Each Division, Business and cross divisional function must maintain a list of individuals who are considered to be IT Leadership for the purpose of this policy.

2. Scope

This policy applies to all WBA employees, contractors and authorized third-parties.

2.1 Policy overview

The GESP is an extension of the Global Information Security Policy ("GISP") and is supported by industry standards and best practices. The content of the GESP is tailored specifically to accommodate all end users throughout the diverse global environment of WBA while the GISP is tailored to WBA technical end users with responsibilities for managing technical systems, applications and data.

The GESP is part of the global policy framework owned and managed by Global IT Governance, Risk & Compliance ("ITGRC"). In addition to the GESP and the GISP, the other WBA IT Global policies that are part of this framework are:

- **Global Security Controls Framework ("GSCF")** which was created as a supporting document to the GISP and establishes the global minimum controls that all WBA entities, IT assets and personnel must comply with. Where local regulations require more stringent controls, it is acceptable that these be implemented locally, however local standards cannot establish weaker security controls than those defined in the GSCF and may not contradict the GSCF. In case of non-compliance with the GSCF controls, a variance must be completed.

- The **WBA Information Technology Policy (IT Policy)** defines the core principles for the management of information technology processes for Walgreens Boots Alliance ("WBA") and to set enterprise wide Information Technology policies, standards and responsibilities that are required to provide alignment across WBA IT divisions, lower operational costs, increase productivity and lower organizational risk. This policy includes IT processes such as system development, change management, problem & incident management, operations and business continuity/disaster recovery.

- The **WBA Information Classification Policy** defines global information classification categories and how they should be assigned to WBA data. IT Leadership or the business must ensure that data stored, processed or transmitted by systems has been classified in accordance with the Information Classification Policy to ensure that appropriate technical and administrative safeguards are applied to protect WBA information.

2.2 Policy compliance

All employees, contractors and authorized third-parties (hereafter referred to as "WBA end users") that handle or have access to WBA facilities, devices, software and information are responsible for ensuring the confidentiality, integrity and availability of all WBA electronic and/or non-electronic information for which they are responsible. Furthermore, employees are also responsible to ensure that authorized third-parties performing services on behalf of WBA follow all applicable policies including, but not limited to the GESP, at all times.

Failure of an employee to follow the GESP may lead to disciplinary procedures in accordance with the WBA Human Resources Policy that correspond with the severity of the failure, up to and including termination of employment. Additionally, authorized third-parties that fail to follow the GESP, may be disciplined up to and including termination of contract.

ITGRC is responsible for maintaining the final version of the GESP and for ensuring compliance with the requirements of the GESP.

WBA end users can ask questions or request policy clarifications by sending an email to GISP@wba.com. In addition, employees can reference the GISP/GSCF for further technical specifications on any topics noted in this policy.

2.3 Policy governance

The GESP is owned and managed by the ITGRC function, which is responsible for any necessary updates to the content of this policy as well as for communication and tracking of GESP compliance.

The GESP will be reviewed periodically as required by the WBA Policy Committee, and following any significant changes to the WBA environment, such as:

- Business needs and environment;
- Legal, statutory, regulatory and contractual obligations;
- External / internal technology environment;
- Emerging technologies;
- Technology and security risks;
- Internal/External audit gaps;
- Requirements or updates from upper management.

3. WBA end User Policy

3.1 Acceptable use

WBA end users have an ongoing responsibility to protect access and all use of WBA technology and information systems. This responsibility applies to WBA business locations, offsite facilities and remote use.

All material created in, transmitted from, received by, or stored in WBA systems must be appropriate, lawful and compliant with WBA IT Policies. WBA information must not be sent or transferred to:

- unauthorized individuals or organizations,
- any online storage site which is not an approved WBA storage solution,
- any personal email accounts.

WBA owned computing devices (such as laptops, desktops, mobile devices), applications (such as business applications, intranet applications, email applications, instant messaging applications), communication systems (such as voice and conferencing), and network resources, (including access to the Internet and other on-line resources), are provided by WBA for the use of its employees and authorized third-parties for business purposes. These systems, devices, applications and networks are the property of WBA and must be used in accordance with WBA policies, professional standards, as well as laws and regulations.

Personal mobile devices, such as laptops, tablets and smartphones, must be approved for business use by IT Leadership. Where applicable, the access and usage of approved personal devices with WBA data must be compatible with the Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standard (PCI–DSS), Sarbanes-Oxley Act (SOX), General Data Protection Regulation (GDPR), and any national and local laws and regulations governing the protection of personal data.

3.2 Personal use

Personal use of WBA technology and information systems including Internet access is permitted as long as the following conditions are met:

- Local management permits it;
- Work performance is not adversely impacted;
- Usage does not cause any disruption or other significant impacts to WBA infrastructure;
- Usage does not interfere or disrupt WBA business operations; and
- All security controls and compliance standards are maintained.

In addition, personal use of WBA technology and information systems including Internet access must be:

- Lawful;
- Not cause additional cost or risk to WBA;
- Not used to solicit non-WBA business for personal gain or profit;

- Compliant with all WBA policies, procedures and standards.

3.3 Privacy and monitoring

Monitoring the use of WBA's information systems and technologies, including Internet access provided by or on behalf of WBA (collectively, "**WBA Information Systems**") is critical to the company for a number of legitimate business purposes, including to:

- Protect against unauthorized use, disclosure or transfer of WBA information classified as Confidential about our employees, customers and service providers;
- Investigate complaints of employee misconduct, including harassment and discrimination complaints;
- Monitor employee compliance with WBA workplace policies related to the use of WBA systems;
- Prevent, detect and/or respond to unauthorized access to WBA systems;
- Protect the performance of WBA systems by preventing unnecessary resource utilization;
- Help prepare WBA's defense to lawsuits or administrative complaints; and
- Satisfy any other legitimate business purpose of WBA as necessary.

Subject to local laws and regulations, policies and representative agreements, WBA may monitor, copy and disclose the usage of WBA systems by end users as necessary to achieve the purposes identified in this policy. This includes the monitoring of all information stored, processed and/or transferred by WBA systems.

Subject to local laws and regulations, policies and representative agreements:

- The monitoring activities described in this notice will be conducted only by WBA personnel and approved service providers who are contractually obligated to protect the information collected through monitoring. Potentially unlawful activities may also be disclosed to employee representatives, works councils, law enforcement or government regulators, as applicable.
- Employees accused of violating applicable WBA policies and procedures shall have the right to respond to such accusation in accordance with WBA's Code of Conduct and Business Ethics.

Your use of WBA systems signifies your consent to the monitoring activities described in this notice.

3.4 Copyrighted materials

Country specific copyright laws protect the intellectual property of WBA materials such as:

- Computer programs,
- Software code,
- Textual materials,
- Audio files,
- Video files,
- Graphics.

WBA end users of WBA equipment or systems are prohibited from copying and/or transmitting any copyrighted material. Questions regarding the potential use of material that is copyrighted must be directed to the WBA Legal Department.

3.5 Device management

WBA systems and information may only be accessed by authorized devices, such as:

- WBA owned desktop and laptop computers or authorized personal laptops/computers,
- WBA owned telephones,
- WBA owned or authorized storage media,
- WBA owned or authorized smart phones and tablets including personal devices authorized by IT Leadership.

WBA end users are required to protect all WBA issued devices and any authorized personal devices with access to WBA systems or information from loss, theft or damage. All lost or stolen devices, including authorized personal devices, must be reported immediately to the local IT Service desk.

WBA end users must take additional precautions to protect devices from unauthorized access or viewing, especially when located outside of a WBA facility. Further, end users are prohibited from changing security settings or deactivating security software on their WBA owned devices.

In addition, WBA end users leaving the Company must return all WBA owned equipment and electronic and non-electronic data to their line managers.

3.6 Software management

WBA end users are prohibited from writing, testing and/or compiling any code (Java, C++, etc.) on WBA devices that are not intended for use for WBA purposes. Additionally, installing software on WBA issued laptops/computers that has not been provided or authorized for business use by WBA is also prohibited. This includes the following actions:

- Downloading software;
- Copying software;
- Modifying software;
- Transferring software;
- Distributing software.

All WBA end users are prohibited from transferring or installing software that was developed and/or licensed by WBA and/or a third party to any other device unless approved by IT Leadership or designee.

WBA end users are allowed to install mobile applications from Reputable application stores on to business issued mobile devices where the software license agreement allows for the use on a business device. WBA end users may not download applications to business issued mobile devices that are not from reputable application stores without consulting with the local IT service desk to ensure they do not pose a security risk to the Company. WBA end users must only use downloaded software applications for individual use without further distribution to another device and in compliance with the respective application's terms of use.

3.7 Data storage

WBA end users must only store WBA information on devices authorized by WBA. The following external storage devices/mechanisms are prohibited without approval from the end user's manager AND IT Leadership or designee which will only be given for exceptional circumstances:

- External storage devices such as flash drives and external hard drives;
- CDs/DVDs;
- Internal and external websites; or
- Any other external storage media not listed above.

External storage devices that are approved by the end user's manager and IT Leadership or designee are required to be virus scanned immediately upon connecting to a WBA issued device. In addition, authorized devices must have the capability to ensure that the following safeguards are met:

All external storage devices or media must be secured at all times, including when the devices or media are not in use;

External storage devices must be encrypted if used to store any Confidential Information;

Data on external storage devices must be erased before disposal or when the device is no longer needed or used.

WBA end users are prohibited from installing and/or utilizing unauthorized Internet based storage solutions for storing and sharing any WBA information. If WBA end users or applications require the use of an Internet based storage solution, they must use a solution that has been approved by IT Leadership and/or provided by WBA.

As required by the WBA Communications Policy (WBA COMMS 1), WBA Communications must approve the initial concept of all new WBA Divisional, Business and Corporate function internal or external websites, including any significant changes to an existing website.

The setting up of a new social media channel is subject to the rules set out in the WBA Social Media Policy (WBA-SM-1).

3.8 Disclosure of Confidential Information and data transfer

WBA end users are prohibited from disclosing, storing, or transmitting Confidential Information to anyone internal or external, who is not authorized to receive the information. Confidential Information is information that WBA has a legal, regulatory or contractual obligation to protect, or, where unauthorized disclosure, compromise, or destruction could result in severe damage, or could have a serious adverse financial and/or reputational impact on WBA, or provide significant advantages to a competitor. Confidential Information includes personal, employee, customer and patient information that is protected by local laws and regulations. Further, Confidential Information must be controlled at all times and must be restricted to individuals who have the need to know.

In the event Confidential Information must be shared with external users or third-parties, the sender must validate the following:

- All recipients are authorized,
- The data is encrypted during transmission, and
- A current, executed Non-Disclosure Agreement ("NDA") or appropriate contracts requiring confidentiality maintained with the external users or third-parties is on file.

WBA end users travelling anywhere in the world with encrypted media or laptops must ensure that they are compliant with all relevant local laws and regulations relating to Confidential Information prior to travelling to the destination country. If anyone has any questions, the local legal department can be contacted for assistance.

WBA end users must also protect electronic and non-electronic documents containing WBA Confidential Information from unauthorized disclosure and/or use by:

- clearing their desk, locking computers and putting documents away before walking away,
- collecting documents from printers immediately,
- shredding confidential documents before disposing them.

3.9 Email

WBA end users are prohibited from intentionally opening email messages, URL links or attachments which are suspicious. Suspicious emails can be "spoofed" or can be part of a "phishing" scam. These messages are purposely made to look like they are from a reliable source – such as a bank or another company and may prompt the users to enter personal information, such as financial, medical or logon details.

In the event an end user receives a message that appears to be suspicious, the end user must ensure the message is not opened and that the local IT Service desk is contacted immediately for further instructions.

WBA end users are prohibited from creating and/or sending messages through WBA email which are, or contain content, as follows:

- Viruses and/or malware;
- Program data that will corrupt, intercept, or hide in existing software or data;
- Initiate or forward emails such as chain letters, mass mailings or any other communication containing material that is:
    - Fraudulent;
    - Sexually explicit;
    - Profane;
    - Obscene;
    - Intimidating;
    - Defamatory;
    - Discriminatory;
    - Unlawful;
    - Inappropriate;

  - “Spam” or “junk mail” - Please note, “spamming” is illegal and is explicitly prohibited by WBA policy; or
  - Unsolicited advertisements or marketing.

3.10 Instant messaging

Only instant messaging programs provided and/or authorized by WBA IT Leadership must be used to communicate WBA Internal Information.

Additionally, the use of instant messaging must comply with sections 3.1 Acceptable Use and 3.2 Personal Use from this policy. Confidential Information must not be communicated via instant messaging. Subject to local laws or regulations, WBA, or an authorized delegate, may inspect, copy, or disclose instant messaging usage at any time with or without notice. WBA reserves the right to disclose non-compliant activity by end users to the end user’s direct manager.

3.11 Security events

It is the user’s responsibility to report suspicious activity (please see examples listed below) to the local IT Service desk. Furthermore, users are prohibited from trying to resolve incidents themselves. Examples of suspicious activities include, but are not limited to:

- Suspicious emails:
- Any signs of possible virus or malware infection;
- Any loss or theft of your WBA issued or approved device (desktop, laptop, storage device, smartphone, tablet, etc.);
- Any unauthorized access to WBA Information.

The response to a data security event is documented in the WBA Data Security EventPlan (DSEP) framework.

The purpose of the DSEP is to establish a global framework, which defines the risk based escalation process, the roles and responsibilities, and protocols for the ongoing communication of the status of a data security event to executive management. No external or internal communications may be made unless instructed to do so by the executive authorized in the DSEP which is available on the WBA Worldwide IT site under IT Policies.

3.12 Password management

Users must adhere to established automated password complexity requirements and automated reminders to change complex passwords on a periodic basis.

While password requirements are enforced by operating system, database or application, an overview of the requirements for 'complex passwords' is listed below. Further, all complex passwords must be compliant with the GISP and GSCF, where technically feasible. At a high level, complex passwords must be:

- A minimum of 7 characters in length;
- At least three of the following four classes: upper and lower case alphabetic characters, numbers, special characters (including punctuation marks or symbols);
- Different to the previous 4 passwords;
- Set to expire every 90 days.

Further, complex passwords must not:

- Be shared by or between users, including co-workers, direct reports, supervisors and administrative assistants*;
- Contain dictionary words without any complexity, common keyboard combinations or publicly available information commonly available on social media sites (e.g. names, birthdays, cities, pets name, kids name, address), which can be easily obtained or guessed by unauthorized users;
- Contain the same character repeated more than twice in sequence;
- Contain associated user ID in any form (as is, reversed, capitalized, doubled);
- Be written down.

*Only WBA Senior Vice Presidents (SVPs) and above may share their password with their administrative assistants for legitimate business purposes for expense reimbursement systems (e.g. Concur and Simple) or non-financial systems where there is no ability to provide the administrative assistant access through their own unique user account. Where this occurs, the

WBA Senior Vice Presidents (SVPs) must provide formally documented guidance of what activities their administrative assistant is allowed to perform. The WBA Senior Vice Presidents (SVPs) will be held accountable for any actions taken by their administrative assistant(s) and must perform sufficient oversight of the administrative assistant's activity to ensure it is only used for approved and legitimate business purposes. Administrative assistants must only use the access that is formally documented. Failure to do so could result in disciplinary action in accordance with the WBA HR Policy.

Complex passwords can be created using a familiar phrase and substituting letters for special characters or numbers. Please see the example below:

- Phrase: **S**ummer **B**reak **i**n **A**malfi **C**oast **'10**
- Characters: $............B........!...@.......c........'!@
- Password: $B!@c'!@

Where systems require a personal identification number (PIN) instead of a password, such as mobile devices and voicemail, the PIN must be complex and a number that is not easily guessable by others. Where systems allow, the PIN must be at least 6 digits long and must not consist of repeating numbers (e.g. 111111) or a sequence of numbers (e.g. 123456).

Only password management tools approved by IT Leadership and/or provided by WBA may be used to manage user accounts and passwords to WBA systems, applications, networks and devices.

Where available, the use of approved biometric technologies is encouraged for users.

3.13 Access management

Managers must only request and approve the minimum access necessary for the user to perform their job function and must ensure that requested access does not conflict with existing access rights and ensures segregation of duties. Managers are also required to change or revoke access that is not necessary in a timely manner. To ensure appropriate access is maintained, managers must review end user access at least annually or more frequently where the level of risk or criticality of a system warrants greater oversight.

NDAs or appropriate contractual terms imposing confidentiality, along with any other agreements required by the Sourcing and/or Legal functions, must be in place for all third-parties with access to WBA systems and information prior to providing access. Divisions, Businesses and the Corporate functions must have in place and keep up to date a list of all third-parties with access to WBA systems.

3.14 End user security awareness

End users are the first line of defense in protecting WBA systems and information. As such, end users are responsible for familiarizing themselves with all end user security awareness guidance, training or documentation provided by WBA and adhering to their requirements in their day-to-day activities. Managers are responsible for ensuring that end users are aware of this policy and comply with its requirements.

3.15 User equipment and active sessions

To prevent unauthorized use, any user equipment that is unattended must be locked by the user activating a suitable method such as password protected screen savers.

3.16 Mobile devices

WBA end users with corporate issued devices must not use their personal device for business purposes unless there is no alternative.

WBA is not obligated to surrender the phone numbers on Corporate devices to the end user.

WBA end users that chose to use their personal device for business purposes must comply with sections 3.1 Acceptable Use and 3.2 Personal Use from this policy.

By choosing to use personal devices for business purposes, the WBA end user may need to surrender their device to WBA to review and/or retain copies of corporate information and business communications on the device to comply with legal, regulatory, and/or policy requirements.

The access of personal mobile devices to WBA systems may be terminated at any time, and, at the sole discretion of WBA.

Further, should a personal or corporate device be lost or stolen, WBA may choose to remotely wipe the device, which removes all data and settings from the device.

3.17 End user computing and storage

Users are responsible for protecting mobile devices, including laptops with WBA information regardless of location. All Confidential Information stored on WBA or WBA authorized computers and devices must be must be handled and protected as outlined in this policy. Further, complex passwords for Technical Custodians or users with privileged access, must be compliant with section 3.12 of this policy and password requirements defined in section 3.4 of the GISP and the GSCF.

WBA has no obligation to recover or turn-over personal data, such as files, email, contacts, music, pictures, or video stored on a corporate device after separation or termination from the company.

3.18 Network and Remote access

WBA end users must not connect any non-WBA equipment or allow third-parties to connect to the WBA network unless authorized by IT leadership.

However, connections to WBA provided *"Guest"* wireless networks (where available) are permissible. Connecting to the WBA network from external wired/wireless networks is permitted only if users are connecting via a solution that has been provided by WBA and/or authorized by IT Leadership (e.g. VPN, Citrix, VDI, etc.).

4. Periodic policy self-assessment

On a periodic basis as requested by the WBA Policy Governance Committee, the Business must complete a Self Assessment Questionnaire (SAQ) which sets out the Business's compliance with this policy.

An action plan with an agreed deadline and identified person(s) responsible to remediate all and any areas of non compliance must be submitted with the SAQ. The Business must provide regular reporting of progress against the remediation plan(s) and ensure non compliance is addressed in a timely manner.

Exhibit A - Glossary

- **Access rights -** Permission granted to users, programs, servers, workstations to create, change, delete, share or view data and files within a system.
- **Applications** – Include, but are not limited to WBA business applications, intranet applications, email applications and instant messaging applications.
- **Authentication** - The process of verifying a claim of identity by a subject in order to confirm that it must be allowed to act on behalf of a given principal (person, computer, process etc.)
- **Authorization** - Verifying the authenticated subject has permissions to perform certain operations or access specific resources. It will be based on company's policies, local laws and regulations as well as best practices.
- **Authorized Devices**– Having an official permission or approval from IT Leadership based on company's policies, local laws and regulations as well as best practices to use devices to be part of WBA network, work with the WBA information or to perform contracted services with WBA and/or WBA subsidiaries if is related to an authorized third-party
- **Availability –** The requirement for an information asset to be available when it is needed.
- **Citrix** – a desktop virtualization software that provides individualized desktops for each user while doing remote access.
- **Communication Systems** - include, but are not limited to WBA voice and conferencing systems.
- **Computing Devices** - Include, but are not limited to approved and authorized desktop computers, laptop computers and mobile devices (unless otherwise specified).
- **Confidential Information –** Information that WBA has a legal, regulatory, or contractual obligation to protect, or, where unauthorized disclosure, compromise, or destruction could result in severe damage, provide significant advantages to a competitor, or incur serious financial impact to Walgreens Boots Alliance. Confidential Information includes, but is not limited to, personal information, employee information, customer information and patient information. Further, WBA Confidential Information must be strictly controlled and restricted only to individuals who have the need to know.
- **Confidentiality** - Preventing the disclosure of information to unauthorized individuals or systems.

- **End user / user(s)** – All WBA employees and third-parties (contractors, consultants, vendors and service providers) that access WBA facilities, systems or networks, and/or process WBA data (electronic or non-electronic).

- **External Storage Devices (or Computer Media) -** An external drive or disk connected in some way to the main computer which can store information, they include, but not restricted to, CD ROM, DVD, USB, iPods, MP3 players, smart phones, tablets.

- **Facilities** - Include, but are not limited to WBA stores, offices, data centers and warehouses.

- **Global Data Protection Regulation (GDPR) -** The GDPR (General Data Protection Regulation) is a regulation by which the European Commission intends to protect EU citizens from privacy and data breaches. It extends the scope of the EU data protection law to all foreign companies processing data of EU residents.

- **HIPAA** - Is the federal Health Insurance Portability and Accountability Act of 1996. The primary goal of the law is to make it easier for people to keep health insurance, protect the confidentiality and security of healthcare information and help the healthcare industry control administrative costs.

- **Information Systems** – A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

- **Integrity** – Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

- **Malware** - Short for "malicious software," malware refers to software programs designed to damage or do other unwanted actions on a computer system. Common examples of malware include viruses, worms, Trojan horses, and spyware.

- **Mobile device** – Laptop, tablet, mobile phone or smart phone, PDA or equivalent.

- **Payment Card Industry Data Security Standard (PCI–DSS) -** PCI security standards are technical and operational requirements set by the PCI Security Standards Council (PCI SSC) to protect cardholder data. The standards apply to all entities that store, process or transmit cardholder data with guidance for software developers and manufacturers of applications and devices used in those transactions.

- **Personal Mobile Devices** – A handheld device that is made for portability so it can be used inside and outside of the company. Some examples are laptops, tablets and smartphones. These devices must be approved for business use by IT.

- **Phishing** – Deceiving individuals into disclosing sensitive personal information through deceptive computer-based means.

- **Remote Access** - The ability for WBA end users to access WBA's network from external locations other than the WBA's facilities.

- **Reputable application stores:** Official application store hosted by the manufacture of the device such as Apple App Store/iTunes, Google Play, Amazon Appstore, Samsung Galaxy Apps, Windows Phone Store**.**

- **Sarbanes-Oxley Act (SOX)** - A United States federal law which established new or expanded requirements for all US public company boards and management to enhance corporate responsibility, financial disclosures and combat corporate and accounting fraud.

- **Secure Wipe** - Also called "secure delete", a method of overwriting data residing on a hard disk drive or other digital media, rendering the data irretrievable.

- **Security Controls** – Safeguards or countermeasures to avoid, mitigate or counteract a security risk.

- **Segregation of Duties (SOD)** –A classic security method to manage conflict of interest, the appearance of conflict of interest, and fraud. It restricts the amount of power held by any one individual. It puts a barrier in place to prevent fraud that may be perpetrated by one individual.

- **Software -** Computer programs and associated data that may be dynamically written or modified during execution. Software types include, but are not limited to HR, financial and accounting applications.

- **Spam –** Electronic junk mail or the abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages.

- **Spoof(ing)** - The deliberate inducement of a user or resource to gain illegal entry into a secure system. Forms of spoofing include impersonating, masquerading, piggybacking, and mimicking.

- **Technical Custodian** - WBA technical end users with responsibilities for managing technical systems, applications and data.

- **User ID** – An account used where there is a requirement to identify the individual interacting with an application, or person responsible for performing an action or processing on a system.

- **Virtual Desktop Infrastructure (VDI)** - The process of running a user desktop inside a virtual machine that is located on a server in the WBA datacenter. Provides security and centralized management by enabling fully personalized desktops for each user.

- **Virtual Private Network (VPN)** – A computer network that uses a public network (Internet) to provide remote offices or individual users with a secure connection to the organization's network.

- **Virus** – A computer program that can copy itself and infect a computer without permission or knowledge of the user. A virus might corrupt or delete data on a computer, use email programs to spread itself to other computers, or even erase everything on a hard disk.

Policy revision history

Version number	Issue Date	Description of changes
Version 1.0	29 April 2016	Initial version
Version 2.0	30 May 2017	• Annual review, updates and publication
Version 2.1	30 May 2017	• Added internal/external websites and this statement to the policy. "As required by the WBA Communications Policy (WBA COMMS 1), WBA Communications must approve the initial concept of all new WBA Divisional, Business and Corporate function internal or external websites, including any significant changes to an existing website. The setting up of a new social media channel is subject to the rules set out in the WBA Social Media Policy WBA-SM-1." Note: since this was an ad-hoc change, the date within the policy stayed the same but the ad-hoc changes happened in November 2017.
Version 3.0	10 December 2018	• clarified accessing internet using WBA equipment is permitted under certain conditions, and additional conditions added (section 3.2); • updated and clarified requirements relating to use of Instant Messaging (section 3.10); • further restricted circumstances under which passwords can be shared (section 3.12); • rewording and simplification of policy relating to employees using personal devices (section 3.16); • updated the requirements when connecting to a WBA network directly or remotely (section 3.18); and • replaced "DCIO or Designee" with "IT Leadership" throughout. (on 29 May 2019) • Updated Contact information

Version 3.1	4 October 2019	Main changes comprise: • adding a new section on Policy Self assessment (section 4); and • updating Contact information

Contact information

Name	Email	Telephone
Michael McGarry, Senior Director, Enterprise Risk Management	michael.mcgarry@wba.com	Office: +847 315 3261 Mobile: +312 860 6090
Preeti V. Gupte Director, WBA IT Governance, Risk & Compliance	preeti.gupte@wba.com	Mobile: +1 2247277143
Mary Ann Bender Manager, WBA IT Governance, Risk & Compliance	maryann.bender@walgreens.com	Office: +1 8479646796 Mobile: +1 8472248271

WBA end users can ask questions or request policy clarifications by sending an email to GISP@wba.com.